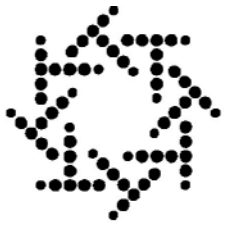

Trusted Information Sharing Network

for Critical Infrastructure Protection

# Critical Infrastructure Protection National Strategy

Version 2.1

12 March 2004

# Contents

## 1. Purpose

This strategy is intended to provide an overarching statement of principles for critical infrastructure protection in Australia, and outline the major tasks and assign responsibilities necessary for their application. This strategy is for use not only by government, but also by the owners and operators of infrastructure, their representative bodies, professional associations, regulators and standards setting institutions.

The strategy provides guidance for the medium term, with a three to five year outlook. It will require detailed implementation plans by governments and industry sectors, and will require the development of interfaces with many other areas of public policy.

## 2. Background

The origin of this strategy lies with the announcement by the Prime Minister in November 2001 of his desire to form a Business–Government Task Force on Critical Infrastructure. The Task Force, which met in March 2002, recommended the establishment of an information-sharing network to continue the business-government partnership. The resulting Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) was launched at the National Summit on Critical Infrastructure Protection on 2 April 2003. In December 2002, the Council of Australian Governments (COAG) endorsed the development by the National Counter-Terrorism Committee (NCTC) of guidelines for critical infrastructure protection, including the establishment of criteria to identify critical infrastructure and the outlining of appropriate security measures. The COAG reinforced the need for a cooperative approach between government and industry and instructed the NCTC to assign priority to the completion of this task due to its national importance. This strategy is intended to continue the work undertaken to date, and provide a common understanding of the issue within all the stakeholder communities.

## 3. Definition

Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security.

For the purposes of this strategy, significant is defined as an event or incident that puts at risk public safety and confidence, threatens our economic security, harms Australia's international competitiveness, or impedes the continuity of government and its services.

Critical infrastructure extends across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services and national icons. Some critical elements in these sectors are not strictly speaking "infrastructure", but are in fact, networks or supply chains that support the delivery of an essential product or service. For example the supply of food to our major urban areas is dependent on some key facilities, but also a complex network of producers, processors, manufacturers, distributors and retailers that get the food from paddock to plate. Where an incident involving these networks could have a significant impact, those networks are treated as critical infrastructure for the purposes of this strategy.

The continuity of supply of all critical infrastructure is dependent, to some extent, on availability of other infrastructure, and some sectors are mutually dependent on each other. The degree and complexity of interdependencies is increasing as Australia becomes more

dependent on shared information systems and convergent communication technologies, including the Internet. Government and the owners and operators of critical infrastructure need to work together to identify these interdependencies and apply appropriate strategies to reduce risk where possible.

## 4. All Hazards

Critical infrastructure can be damaged, destroyed or disrupted by natural disasters, negligence, accidents or by deliberate acts of terrorism, computer hacking, criminal activity and malicious damage. While terrorism has assumed a higher profile in Australia's current threat environment, our critical infrastructure has to be protected against all threats and hazards presenting a risk to the continuity of service.

## 5. Scope of critical infrastructure protection

Not all infrastructure can be protected from all threats. For example, electricity transmission networks are too large to fence or guard. By applying risk management techniques, attention can be focused on areas of greatest risk, taking into account the threat, relative criticality, the existing level of protective security and the effectiveness of available mitigation strategies for business continuity.

Critical Infrastructure Protection (CIP) is not a new discipline, but is a coordinated blending of existing specialisations, including:

- law enforcement and crime prevention
- counter terrorism
- national security and defence
- emergency management, including the dissemination of information
- business continuity planning
- protective security (physical, personnel and procedural)
- e-Security
- natural disaster planning and preparedness
- risk management
- professional networking
- market regulation, planning and infrastructure development.

CIP brings together a significant number of existing strategies, plans and procedures that deal with the prevention, preparedness, response and recovery arrangements for disasters and emergencies.

In some parts of Australia as much as 90% of critical infrastructure is privately owned. As such, CIP cannot be carried out solely by government. Individual companies may not have the information or resources to assess or mitigate the risks from a whole-of-sector perspective. To achieve success, industry and government at all levels need to work together to raise awareness of infrastructure security risks across the nation and ensure that information and techniques required to assess and mitigate risks is readily available and freely exchanged.

## 6. Identification of critical infrastructure

Any risk assessment of critical infrastructure will begin by establishing a strategic context relevant to the community or sector concerned. Therefore each sector and government will need to identify infrastructure critical to their mission. State and Territory governments will identify critical infrastructure within their respective jurisdictions, with the Australian Government identifying those elements of our critical infrastructure which are Federally regulated, support national security and defence, the continuity of government, the delivery of its services and any infrastructure of additional national importance. Sectors will need to identify infrastructure that is vital to the on-going continuity of supply to the community, particularly those that exhibit high vulnerability, or where there is mutual dependence across the sector. The identification of critical infrastructure is an ongoing process and regular review will be required to keep abreast of changes, both physical and logical (both process related and IT), the ever increasing dependency of the community and interdependencies between infrastructures.

## 7. Principles of Critical Infrastructure Protection

CIP requires the active participation of the owners and operators of infrastructure, regulators, professional bodies and industry associations in cooperation with all levels of government, and the public. To ensure this cooperation and coordination all of these participants should commit to the following set of common fundamental principles of CIP. These principles are to be read as a whole, as each sets the context for the following.

1. CIP is centred on the need to minimise risks to public health, safety and confidence, ensure our economic security, maintain Australia's international competitiveness and ensure the continuity of government and its services.
2. The objectives of CIP are to identify critical infrastructure, analyse vulnerability and interdependence, and protect from, and prepare for, all hazards.
3. As not all critical infrastructure can be protected from all threats, appropriate risk management techniques should be used to determine relative criticality, the level of protective security, set priorities for the allocation of resources and the application of the most efficacious mitigation strategies for business continuity.
4. The responsibility for managing risk within physical facilities, supply chains, information technologies and communication networks primarily rests with the owners and operators.
5. CIP needs to be undertaken from an 'all hazards approach' with full consideration of interdependencies between businesses, sectors, jurisdictions and government agencies.
6. CIP requires a consistent, cooperative partnership between the owners and operators of critical infrastructure and governments.
7. The sharing of information relating to threats and vulnerabilities will assist governments, and owners and operators of critical infrastructure to better manage risk.
8. Care should be taken when referring to national security threats to critical infrastructure, including terrorism, so as to avoid undue concern in the Australia domestic community, as well as potential tourists and investors overseas.
9. Stronger research and analysis capabilities can ensure that risk mitigation strategies are tailored to Australia's unique critical infrastructure circumstances.

## 8. Achieving a business-government partnership

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) enables the owners and operators of critical infrastructure to share information on important issues such as business continuity, consequence management, information system attacks and vulnerabilities, e-crime, protection of key sites from attack or sabotage, chemical, biological and radiological threats to water and food supplies, and the identification and protection of offshore and maritime assets. The TISN comprises a number of Infrastructure Assurance Advisory Groups (IAAGs) for different business sectors, and will network with like groups overseas.

The Critical Infrastructure Advisory Council (CIAC) forms part of the TISN. It oversees the IAAGs and provides advice to the Attorney-General on the national approach to protecting critical infrastructure. The CIAC consists of representatives from each of the critical infrastructure business sectors, each of the States and Territories, relevant Australian Government agencies and the National Counter-Terrorism Committee. The CIAC is chaired by the Attorney-General's Department of the Australian Government (AGD). The CIAC will concentrate on the medium-to-long-term issues concerned with the prevention, preparedness and recovery aspects of CIP, particularly those matters requiring coordination with the private sector. The CIAC will also assist in identifying research issues requiring priority attention.

## 9. Coordination within and between Australian governments

Institutional arrangements will be necessary to coordinate the activities of the Australian Government in CIP with those of the States and Territories. For this reason the National Counter-Terrorism Committee and the State and Territory Governments are members of the CIAC.

In order to facilitate the discussion, development, coordination and implementation of CIP policy, a number of committees have been established:

The National Committee on Critical Infrastructure Protection (NCCIP) is the formal standing committee to coordinate CIP policy development across all levels of government. The committee comprises the Australian and State/Territory government representatives on the CIAC as well as representatives from the Australian Local Government Association, the Australian Security Intelligence Organisation, the Department of Defence, the National Office for the Information Economy and any other agencies wishing to participate. Issues to be considered by the committee will include inter-governmental issues related to CIP.

The Information Infrastructure Protection Group (IIPG) is an Australian Government interdepartmental committee responsible for providing policy coordination and/or technical response in relation to threats to the National Information Infrastructure (NII).

## 10. Information sharing

The sector IAAGs have been created to allow the owners and operators of critical infrastructure to share information on shared threats and vulnerabilities and appropriate measures and strategies to mitigate risk. The participation of government agencies in the sector groups will assist in a greater understanding of issues by the government, and allow industry to be briefed on government activity. AGD will assist sector groups in the TISN to collaborate on issues of common threat or vulnerability, and interdependence.

ASIO, as the national threat assessment agency, prepares assessments of the likelihood and probable nature of acts of politically motivated violence and other acts prejudicial to

security. ASIO distributes threat assessments to relevant Australian Government departments and agencies and to the AFP and State and Territory police. Threat assessments relating to critical infrastructure fall into two broad categories, those that:

- assist preparedness and planning; or;
- require an immediate response either to a specific threat or a heightened assessment of threat.

ASIO will identify the information in threat assessments that is releasable to the private sector and to government agencies where security clearances are not held by recipients.

State and Territory governments have responsibility to coordinate a whole-of-government process that ensures the relevant information is passed to all relevant government departments and agencies, including emergency services organisations, and affected owners and operators of critical infrastructure and local governments, through a network of contacts established within the States and Territories.

Australian Government liaison officers have responsibility for informing relevant industry peak bodies of the relevant information. Existing forums and mechanisms should be used for information distribution as far as possible.

While some overlap may occur in some elements of information being passed from industry peak bodies to their constituency and the mechanisms within States and Territories, this potential duplication is preferable to the possibility that information might not be passed to some owners and operators of critical infrastructure.

It is recognised that information sharing regarding critical infrastructure protection needs to take place in an environment of trust and confidentiality. As discussions in the TISN could involve the disclosure of confidential information, it is desirable to have in place an appropriate framework to ensure that confidential information is properly managed and reasonably protected from unauthorised use or disclosure. The TISN Deed of Confidentiality provides a "safety net" to facilitate the creation of an environment of trust and transparency by providing guidelines for the handling of potentially commercially sensitive and security-related information.

## 11. Response to predominant threats and risks

Whilst the National Strategy is aimed at addressing medium to long-term requirements, from time to time specific risks or threats may emerge that require an immediate national response, i.e. terrorism. On these occasions a well-coordinated but more operationally focused response will be required from governments and industry. In these circumstances the Australian Government will usually take a lead role in coordinating the development of specific responses, and detailed supporting arrangements will be agreed with stakeholders on a case-by-case basis.

## 12. Relationship with the national counter terrorism arrangements

Governments and industry have recognised and agreed to develop some immediate measures and procedures to counter the heightened threat of terrorism to critical infrastructure. The National Counter Terrorism Committee has been tasked to work with governments and industry to address this issue. The role of the National Counter Terrorism Committee (NCTC) in CIP is to ensure a national strategy is developed and maintained for the coordination of the protection of critical infrastructure from terrorism. This is reflected in the National Counter Terrorism Plan and the National Counter Terrorism Handbook.

The NCTC will include CIP as a theme in counter terrorism training and exercises, and will consider specialist capabilities for responders to work in and around critical infrastructure.

## 13. Responsibilities

Responsibility for implementing this strategy is shared amongst the participants. The following provides an outline of these responsibilities:

Australian Government

- provides strategic leadership, coordination in development and implementation of a nationally consistent approach to the protection of critical infrastructure;
- provides coordination and national leadership in areas of joint responsibility;
- liaises with and supports State and Territory governments in critical infrastructure protection arrangements;
- ensures protection of essential Australian Government services, for example defence establishments, foreign missions, Parliament House, etc;
- communicates relevant intelligence and information to stakeholders;
- ensures that protective arrangements are in place for Australian Government regulated sectors;
- ensures that protective arrangements are in place to protect offshore assets and multi-jurisdictional critical infrastructure;
- develops and maintains a database of nationally significant critical infrastructure;
- coordinates liaison with overseas governments on CIP issues;
- communicates required information to international organisations in accordance with treaty obligations;
- promotes CIP as a national research priority;
- assists owners and operators of critical infrastructure in Australian Government regulated sectors with the development, validation and audit of relevant plans;
- promotes the need for investment in resilient, reliable infrastructure with market regulators;
- strengthens national capacity to safeguard information security, including the research and development and skills base, and;
- manages and coordinates public information and the media at a national level.

State and Territory governments

- provide leadership and whole-of-government coordination in developing and implementing the nationally consistent approach to the protection of critical infrastructure within their jurisdictions;
- develop consequence management and community recovery capacities;
- work with the owners and operators to encourage them to develop relevant capabilities to protect the critical infrastructure and so ensure continuity of service;

- identify and maintain a database of critical infrastructure in their jurisdictions;
- ensure appropriate protective arrangements are in place to protect essential State/Territory government services, for example government utilities and key government facilities;
- develop and communicate on a jurisdictional basis with owners and operators of critical infrastructure the agreed type of response expected for each level of threat/alert;
- assist owners and operators of critical infrastructure with the development, validation and audit of relevant plans;
- liaise with and support the Australian Government in CIP arrangements;
- communicate relevant intelligence and information to stakeholders, and;
- manage and coordinate public information and the media within the jurisdictions.

National Counter Terrorism Committee

- develops and maintains a national strategy for the coordination of the protection of critical infrastructure from terrorism;
- ensures that national counter-terrorism exercises include significant elements of the critical infrastructure; and
- advises the CIAC of its priorities and issues of concern.

State and Territory police

- assist in the provision of protective security advice and develop protective security strategies to counter terrorism;
- advise critical infrastructure owners and operators of relevant threat information, in accordance with jurisdictional arrangements;
- ensure liaison is established and maintained with critical infrastructure owners and operators;
- ensure that intelligence is gathered and disseminated to relevant agencies, and;
- conduct and participate in exercises involving critical infrastructure.

Local Governments

- provide local leadership and community based coordination in implementing the nationally consistent approach to the protection of critical infrastructure at the local level;
- promote the importance of critical infrastructure protection within local communities;
- support critical infrastructure protection arrangements, where necessary, through the exercise of planning and land use powers, building and infrastructure design regulations, and the development assessment process;
- work with owners and operators to ensure critical infrastructure protection plans include appropriate linkages with local stakeholders;

- support the strengthening of consequence management and community recovery capacity through locally coordinated critical infrastructure protection frameworks.

Owners and operators of critical infrastructure

- provide adequate security of their assets;
- actively apply risk management techniques to their planning processes;
- conduct regular reviews of risk management assessments and plans;
- report any incidents or suspicious activity to State or Territory police;
- develop and regularly review business continuity plans; and
- participate in any exercises to test plans conducted by government authorities.

The Critical Infrastructure Advisory Council

- provides policy advice to the Attorney-General on the national approach to critical infrastructure protection;
- provides oversight to the Trusted Information Sharing Network (TISN) for critical infrastructure protection, and;
- considers issues raised by sectors groups in the TISN, particularly where they touch on sector interdependency.

Professional bodies

- should promote CIP within their professions, and assist in the development of guidelines, best practice standards and information sharing.

Regulators

- should consider the need for investment in resilient, robust infrastructure in market regulation decisions.

Standards Australia International

- should promulgate standards on risk management, corporate governance, business continuity and security.

## 14. Research

Targeted research which aims to provide practical strategies or tools for risk mitigation is of prime importance to securing Australia's critical infrastructure in the medium to long-term. The demand for research will only increase as the number of infrastructure dependencies increase.

## 15. Public information

In addition to specific media releases and speeches, information on the TISN and CIAC will be published on the Critical Infrastructure Protection web site (www.tisn.gov.au) or requested by emailing cip@ag.gov.au.

National security information from the Australian Government can be found on the National Security website: www.nationalsecurity.gov.au

## 16. Measurable objectives

The goal of CIP is to ensure that there are adequate levels of protective security on critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements.

CIP is an ongoing process and regular review will be required to keep abreast of the issues and concerns within the community. Success will be measured by:

- governments having identified critical infrastructure in their jurisdictions;
- CIP being a feature of the plans and exercises of counter terrorism, emergency response and business continuity arrangements;
- the need for investment in resilient, robust infrastructure being considered in market regulation decisions;
- businesses collaborating within sectors and with government to share information, and taking steps to reduce the likelihood of a single incident causing widespread or lengthy disruption to critical infrastructure;
- businesses and governments collaborating to identify key interdependencies and vulnerabilities with respect to both cyber and physical infrastructure;
- governments having implemented adequate substantive and procedural laws, and trained personnel, to enable them to investigate and prosecute attacks on critical infrastructure;
- businesses and governments collaborating to promote national research and development in CIP;
- governments having created mechanisms to distribute intelligence, alerts and share information relating to critical infrastructure, and;
- businesses and governments collaborating to develop and promote best practice in mitigating risks to critical infrastructure.

## 17. The role of regulation

Experience in other countries indicates that even when the threat of terrorism is high, business does not always accept the need to invest in infrastructure protection against terrorism. The all-hazards approach however, offers a greater justification for business investment as it mitigates the risk of other less severe, but more likely, threats. As many of the mitigation strategies are identical, particularly in business continuity planning, then CIP from an all-hazards approach should achieve the desired outcome and at the same time provide business with a range of benefits from reduced risk. Regulation may be considered however if the business-government partnership fails to adequately protect critical infrastructure

## 18. Implementation

Each group of stakeholders will need to develop and maintain implementation plans for CIP, based upon or in alignment with this strategy. Within each sector there is a need for collaboration by business and government to define and identify critical infrastructure, with particular emphasis to elements displaying higher vulnerabilities and those that are

crucial for the continuity of supply of multiple providers. The different sectors will then need to work together to gain a better understanding of interdependencies and how this might affect business continuity planning. Sectors will also need to identify their needs for research and standards to assist in risk mitigation.

Governments will need to identify critical physical and information infrastructure relevant to their jurisdiction and internal operations, and how other areas of public policy inter-react with CIP policy. This would include assisting industry sectors with understanding the threat and consequence variables in their risk assessments. Law enforcement and the emergency management community should ensure that CIP is an integral part of their planning and awareness raising. The National Counter Terrorism Committee should include CIP as part of its planning and exercise activities.